UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/716,588	11/19/2003	Minwen Ji	200311664-1	6293

22879 7590 12/19/2006

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/19/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/716,588	JI ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 November 2003* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Thanhnga B. Truong
AU2135

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/19/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the communication filed on November 19, 2003. Claims 1-18 are pending. At this time, claims 1-18 are rejected.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. The claimed invention is directed to non-statutory subject matter.

a. *Referring to claim 1:*

i. This claim consists a method for calculating a message authentication function. The claim purely recites the mathematic calculation. Thus, it is an abstract idea, directed solely to non-functional descriptive material. Therefore, claim 1 recites a non-statutory subject matter. Claims 2-8 have limitations that are similar to those of claim 1, thus they are rejected with the same rationale applied against claim 9 above.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Ripley et al (US 2002/0087818 A1).

a. *Referring to claim 1:*

i. Ripley teaches a method, comprising:

(1) calculating a first part of a message authentication function by a first processor **(see Figure 4 and more details in paragraph 0055 of Ripley);**

(2) calculating a second part of the message authentication function by a second processor **(see Figure 4 and more details in paragraph 0056 of Ripley);** and

(3) combining the results of the first and second parts into the message authentication code by the first or second processors **(see Figure 4 and more details in paragraph 0057 of Ripley).**

b. *Referring to claim 2:*

i. Ripley further teaches:

(1) wherein the message authentication function is used, in part, to authenticate data transmitted between the first processor and a third processor **(see Figure 4 and more details in paragraph 0058 of Ripley).**

c. *Referring to claim 3:*

i. Ripley further teaches:

(1) wherein the first and second processors are provided in separate computer systems **(see Figure 4 and more details in paragraph 0058 of Ripley).**

d. *Referring to claim 4:*

i. Ripley further teaches:

(1) wherein the first and second parts of the message authentication function consist of one-way hash functions **(paragraph 0074 of Ripley).**

e. *Referring to claim 5:*

i. Ripley further teaches:

(1) wherein calculating the first part comprises calculating a value without having a data key associated with the function **(paragraph 0075 of Ripley).**

f. *Referring to claim 6:*

i. Ripley further teaches:

(1) wherein calculating the second part comprises calculating a value for a data set without having contents of the data set **(paragraph 0075 of Ripley).**

g. *Referring to claim 7:*

i. Ripley further teaches:

(1) storing the contents into a non-volatile memory coupled to the first processor and storing the message authentication code into non-volatile memory coupled to the second processor **(paragraphs 0042 and 0044 of Ripley).**

h. *Referring to claim 8:*

i. Ripley further teaches:

(1) calculating a message authentication code using the message authentication function on a data set, wherein the message authentication code can be used to authenticate a record that consists of the data set **(paragraphs 0055-0058 of Ripley).**

i. *Referring to claim 9:*

i. Ripley teaches a method implemented in a first computer, comprising:

(1) creating a record **(paragraphs 0029 and 0072 of Ripley);**

(2) computing a first part of a message authentication function using the contents of the record **(see Figure 4 and more details in paragraph 0055 of Ripley);**

(3) providing the result of the first part to a second computer **(see Figure 4 and more details in paragraph 0056 of Ripley);** and

(4) receiving the result of a second part of the message authentication function from the second computer, said second part computed using a data key that is not available to the first computer **(see Figure 4 and more details in paragraph 0057 of Ripley).**

j. *Referring to claim 10:*

i. Ripley further teaches:

(1) encrypting the record and transmitting the record to a third computer **(paragraph 0059 of Ripley).**

k. *Referring to claim 11:*

i. This claim has limitations that is similar to those of claims 1 and 9, thus it is rejected with the same rationale applied against claims 1 and 9 above.

l. *Referring to claim 12:*

i. This claim has limitations that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

m. *Referring to claim 13:*

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

n. *Referring to claim 14:*

i. This claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

o. *Referring to claim 15:*

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

p. *Referring to claim 16:*

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

q. *Referring to claim 17:*

i. Ripley teaches a computer, comprising:

(1) a processor **(paragraph 0029 of Ripley);** and

(2) memory containing code executable by said processor **(paragraph 0023 of Ripley);**

(3) wherein said executable code causes said processor to compute a first part of a message authentication function including contents of a record, providing the result of said first part to a second computer, receiving the result of a second part of the message authentication function from the second computer, and encoding the record with the result of the second par **(paragraph 0059 of Ripley);** and

(4) wherein the record contents are not revealed to the second computer and the second part is computed by the second computer using a data key that is not revealed to the first computer **(paragraph 0075 of Ripley).**

r. *Referring to claim 18:*

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Tomkow et al (US 2003/0172120 A1) discloses a first party (e.g. educational testing service) provides through the internet to a control server information (e.g. test server) relating to a second party (e.g. a student taking tests prepared by the service). The server provides and may store a verification (e.g. an encrypted digital signature) of, but does not store, the second party information. The server transmits the information and the verification through the internet to the second party. The second party transmits to the server through the internet the information and the verification with a request to transmit the information to a designated third party (e.g. a college or university to which the student has applied for admission). The server authenticates the information through verification comparisons (or through comparison of the information with the reconstruction and decryption of the verification) and transmits the information, authenticated by the server and the testing service, to the third party (see abstract).

b. Mattox et al (US 2004/052377 A1) disclose an apparatus and a receiver, which is in a broadband communication system, includes the logic necessary for protecting keys used for encrypting content that is received by the receiver. The apparatus validates the keys and denies the receiver the use of the keys if they become invalid (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Thanhnga B. Truong
AU2135

TBT
December 4, 2006